

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



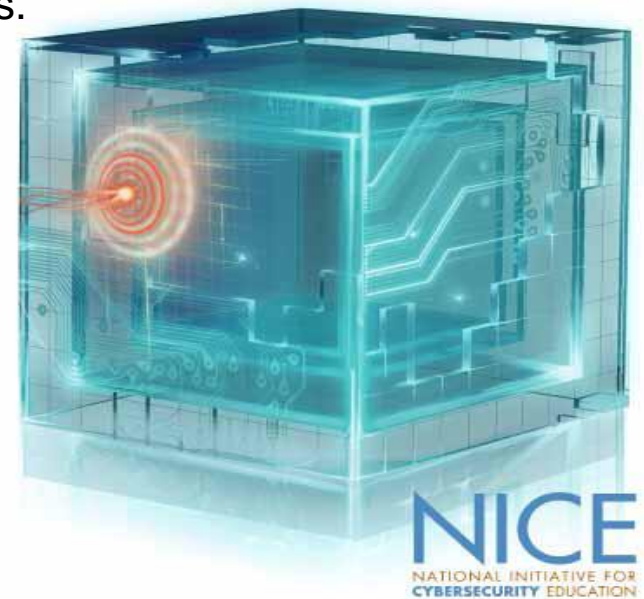
National Initiative for Cybersecurity Careers and Studies (NICCS)

Cybersecurity Training and Education Catalog
Training Provider Instruction Guide

Overview

During this presentation, you will:

- Learn about the National Initiative for Cybersecurity Education (NICE), and one of its implementation tools, the National Initiative for Cybersecurity Careers and Studies (NICCS). The NICCS Portal is a public-facing website accessible to the Nation.
- Explore the Cybersecurity Training and Education Catalog, which provides a comprehensive resource of cybersecurity training.
- View the catalog from the user and trainer perspectives.
- Understand the process needed to add your organization's own training to the catalog.
- Obtain NICCS contact information so you can submit courses, provide feedback, and ask any questions.



Cyber Threats Increase Every Day

As a Nation, we must respond by not only improving our technical infrastructure, but also by developing and maintaining a highly skilled cyber workforce capable of protecting our networks against cyber attacks.

- In May 2009, the President ordered a Cyberspace Policy Review to develop a comprehensive approach to secure and defend America's infrastructure. The review built upon the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in 2008.
- In this presentation, you will learn about an initiative that expanded from CNCI – the **National Initiative for Cybersecurity Education (NICE)** – and its goals to improve the Nation's cybersecurity workforce.
- You will also learn about a tool in development to support those goals. This is the **Cybersecurity Training and Education Catalog** which provides a comprehensive cybersecurity training repository.



Formation of NICE

In response to increased cyber threats across the Nation, the National Initiative for Cybersecurity Education (NICE) expanded from a previous effort, the Comprehensive National Cybersecurity Initiative (CNCI) #8.

- NICE formed in March 2011, and is a nationally-coordinated effort comprised of over 20 federal departments and agencies, and numerous partners in academia and industry.
- NICE focuses on cybersecurity awareness, education, training and professional development.
- NICE seeks to encourage and build cybersecurity awareness and competence across the Nation and to develop an agile, highly skilled cybersecurity workforce.



Cybersecurity Workforce Defined

Version 1.0 of the National Cybersecurity Workforce Framework was published in August 2012, and provides a common lexicon for understanding cybersecurity work. It outlines 31 cybersecurity specialty areas describing functional work.

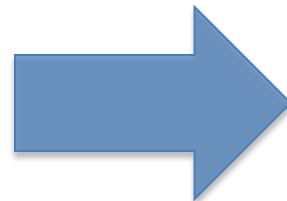
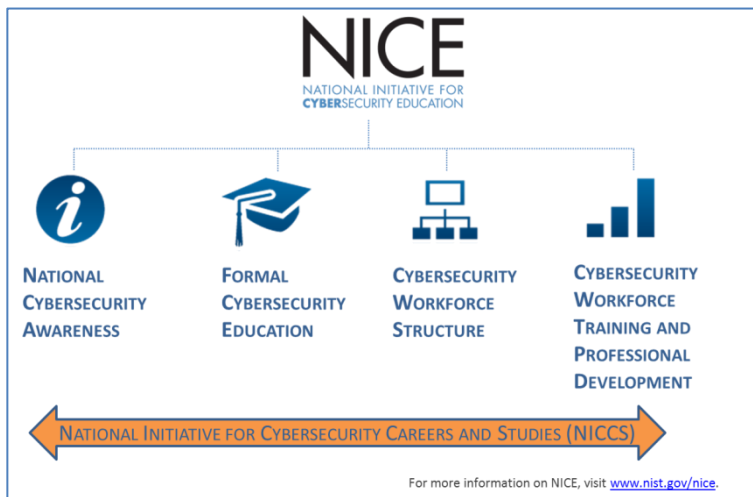
- The Framework was developed in collaboration with subject matter experts from government, non-profits, academia, and the private sector.
- The Framework organizes cybersecurity work into seven high-level cybersecurity categories, each comprised of multiple specialty areas.
- It defines and standardizes cybersecurity roles. Creating consistency in the language used to describe cybersecurity work is an essential step in ensuring the Nation can educate, recruit, train, and develop a highly-qualified workforce.
- Going forward, cybersecurity workforce recruitment, professional development, and talent deployment will be aligned to the Framework.



CYBERSECURITY
WORKFORCE
FRAMEWORK

National Initiative for Cybersecurity Careers and Studies (NICCS) Portal

The NICCS Portal is a national online resource for cybersecurity awareness, education, talent management, and professional development and training. NICCS Portal is an implementation tool for NICE. Soft launched in December 2012, its mission is to provide comprehensive cybersecurity resources to the public.



Visit NICCS here: <http://niccs.us-cert.gov/>

NICCS Goals and the Portal

The vision of NICCS is to serve as the Nation's online resource to learn about cybersecurity awareness, education, careers, and workforce development opportunities.

Goal 1: Build a National Cybersecurity Resource

- Elevate cybersecurity awareness and encourage the public to adopt a culture of cyberspace security.

Goal 2: Promote Cybersecurity Education

- Nurture the future cybersecurity workforce by promoting kindergarten through post graduate level education
- Build an **online community** for cybersecurity professionals and others to gain knowledge related to their field.

Goal 3: Guide Cybersecurity Standards

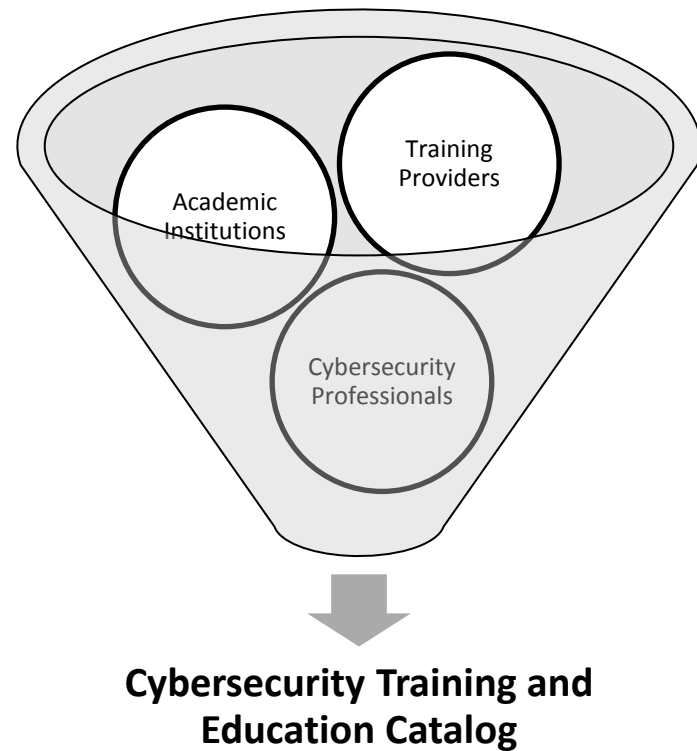
- Guide the development of cybersecurity standards, training, and professional development to empower and advance cybersecurity personnel.

Cybersecurity Training and Education Catalog

To promote cybersecurity education, and to provide a comprehensive resource for the Nation, NICE developed the Cybersecurity Training and Education Catalog. The Cybersecurity Training and Education Catalog will be hosted on the NICCS Portal.

Benefits of the Cybersecurity Training and Education Catalog include the following:

- Brings together cybersecurity professionals, training providers, and academic institutions in an interactive online environment.
- Provides a repository of cybersecurity knowledge and a one stop shop for all types of cybersecurity training.
- Allows the general public to easily and quickly access cybersecurity training suited to their needs.



Benefits of the Catalog

Additionally, the development of the Cybersecurity Training and Education Catalog offers many benefits to training providers and cybersecurity professionals:

- Training providers can map their cybersecurity training to the National Cybersecurity Workforce Framework.
- Training providers can offer courses more tailored to the needs and requirements of cybersecurity professionals.
- Training providers can promote their cybersecurity training.
- Cybersecurity professionals can precisely search for training based on Framework Specialty Area.

NOTE: While the Department of Homeland Security (DHS) strives to make the information on the Cybersecurity Training and Education Catalog as timely and accurate as possible, DHS makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the contents of the Cybersecurity Training and Education Catalog, and expressly disclaims liability for errors and omissions in the contents of the Cybersecurity Training and Education Catalog.

Navigating the Catalog: Getting Started

You can navigate the Cybersecurity Training and Education Catalog in the following ways:

- Search the Cybersecurity Training and Education Catalog by course;
- Explore the Framework;
- Search for courses by Framework Specialty Area;
- Search by Keyword or Training Provider.

Additionally, you can submit training information to be added to the Cybersecurity Training and Education Catalog.



Lets look at how to navigate the Cybersecurity Training and Education Catalog and learn how to submit your training information...

Navigating the Catalog: Access

The screenshot shows the NICCS (National Initiative for Cybersecurity Careers and Studies) website. The top navigation bar includes links for HOME, AWARENESS, EDUCATION, **TRAINING** (highlighted with a red circle), CAREERS, NEWS & EVENTS, COMMUNITY, and RESEARCH. Below the navigation bar, the 'TRAINING' section is titled 'Promoting Continuous Workforce Development'. On the left, a sidebar menu lists: Training Home, National Cybersecurity Workforce Framework, **Training Catalog** (highlighted with a red circle), Call for Providers, Map Your Training, Professional Certifications, FedVTE and FedCTE, and Workforce Development. The main content area features several tiles: 'FIND COURSES' (highlighted with a red circle), 'EXPLORE CERTIFICATIONS', 'TRAINING RESOURCES FOR FEDERAL EMPLOYEES', 'ASSESS & PLAN', and 'SUBMIT TRAINING'. Red arrows point from the 'TRAINING' tab in the navigation bar to the 'Training Catalog' link in the sidebar, and from the 'FIND COURSES' tile to the 'Training Catalog' link in the sidebar.

To access the Cybersecurity Training and Education Catalog, click on the **TRAINING** tab. It's the 4th tab from the left.

On the training landing page, you can click either **"Training Catalog,"** or the **"Find Courses"** button to enter the catalog.

Other links on this page will allow you to learn more about the Framework, and explain how to submit your training courses.

Why promote Cybersecurity training?

Securing, protecting, and defending our Nation's digital information and associated systems and infrastructure require building and retaining an agile, highly skilled workforce that can respond flexibly to dynamic requirements. This is one of the foundational goals of the National Initiative for Cybersecurity Education (NICE). Building our nation's **cybersecurity** workforce requires two complementary components: workforce planning and professional development. Workforce planning entails analyzing the

Navigating the Catalog: Training Search

To search the Training Catalog, click on the **Catalog Search** Tab.

Cyber Professionals can use the Training Catalog to search available courses by **Specialty Area, Keyword, Provider**.

Training can also be browsed using the interactive Framework Specialty Areas by clicking **Browse Courses using the Workforce Framework**.

Navigating the Catalog: Training Search

The screenshot shows the NICCS website's Training Search interface. The navigation bar includes links for HOME, AWARENESS, EDUCATION, TRAINING, CAREERS, NEWS & EVENTS, COMMUNITY, and RESEARCH. Below the navigation bar, there's a search bar and a 'Results' tab. The main content area displays a list of training courses. The first course, '7 Day CISSP Boot Camp InfoSec Institute', is highlighted with a red circle and a red arrow pointing to it. The left sidebar contains filter options for 'Refine Course Criteria', 'by Specialty Areas', and 'by Provider'.

Education and Training Catalog Search Explore the Framework

Catalog Introduction Try Our Demo Results

Records: 59 | Showing 1-10 | [+]

Filter Search

Refine Course Criteria

Keyword filter

by Specialty Areas

--Select one or more specialty areas--

Technology Research and Development

Test and Evaluation

Vulnerability Assessment and Management

by Provider

--Select one or more providers--

Academic Institution D

Government Organization B

Government Organization C

Reset Filter

7 Day CISSP Boot Camp InfoSec Institute
Vendor I

InfoSec Institute provides this highly-rated 7 Day CISSP Boot Camp to the Information Security community. The CISSP Boot Camp trains and prepares you to pass the premier security certification, the Certified Information Systems Security Professional (CISSP). Professionals that hold the CISSP have...

Advanced Security Essentials - Enterprise Defender
Vendor O

Cyber security continues to be a critical area for organizations and will continue to increase in importance as attacks become stealthier, have a greater financial impact on an organization, and cause reputational damage. While Security Essentials lays a solid foundation for the security...

Building Secure Software
Vendor B

Provides a solid understanding of the concepts and techniques underlying the design and implementation of secure software. This class is language neutral, but can be customized to the programming language of choice.

Catching the Hackers - Intro to Intrusion Detection Systems
Vendor Q

This three-day seminar investigates the strengths and weaknesses of network- and host-based intrusion detection systems (IDS). You will explore the leading IDS products on the market today, including Cisco NetRanger, ISS RealSecure, NFR - Network Flight Recorder, Shadow (freeware), Tripwire...

Catching The Hackers II: Systems to Defend Networks
Vendor Q

After submitting a certain search request, a listing of all courses matching the specific criteria will be displayed.

Click on one of the course names to learn more about that training.

Navigating the Catalog: Training Course Description

Training > Training Catalog > Search

THE TRAINING CATALOG

[Catalog Search](#) [Explore the Framework](#)

[Return to Search](#)

Telecommunications in Information Systems

[Learning Objectives](#) | [Available Sessions](#) | [Framework](#)

Description
An analysis of technical and managerial perspectives on basic concepts and applications in telecommunication systems. An overview of data communication protocols and standards; local area networks, wide area networks, and internetworks; and trends in telecommunications is provided. The implications of the regulatory environment and communications standards on transmission of voice, data, and image are examined.

Course Prerequisites : CSIA 301 Information System Architecture
Training Purpose : Continuing Education, Skill Development, Functional
Overall Course Level : Intermediate
Specific Audience:
Training Origin : Academic Institution

Learning Objectives

- Obtain an understanding of the overview of data communication protocols and standards; local area networks, wide area networks, and internetworks; trends in telecommunications; and the implications of the regulatory environment and communications standards on transmission of voice, data, and image.

This Course Fulfills the following KSAs

- Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools
- Knowledge of network architecture concepts including topology, protocols, and components
- Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services
- Knowledge of network security architecture, including the application of Defense-in-Depth principles
- Knowledge of network traffic analysis methods
- Knowledge of Open System interconnection model
- Knowledge of packet-level analysis
- Skill in protecting a network against malware
- Skill in securing network communications
- Skill in using VPN devices and encryption

Categories:

- Analyze
- Investigate
- Operate and Collect
- Operate and Maintain
- Protect and Defend
- Securely Provision
- Support

Competencies:

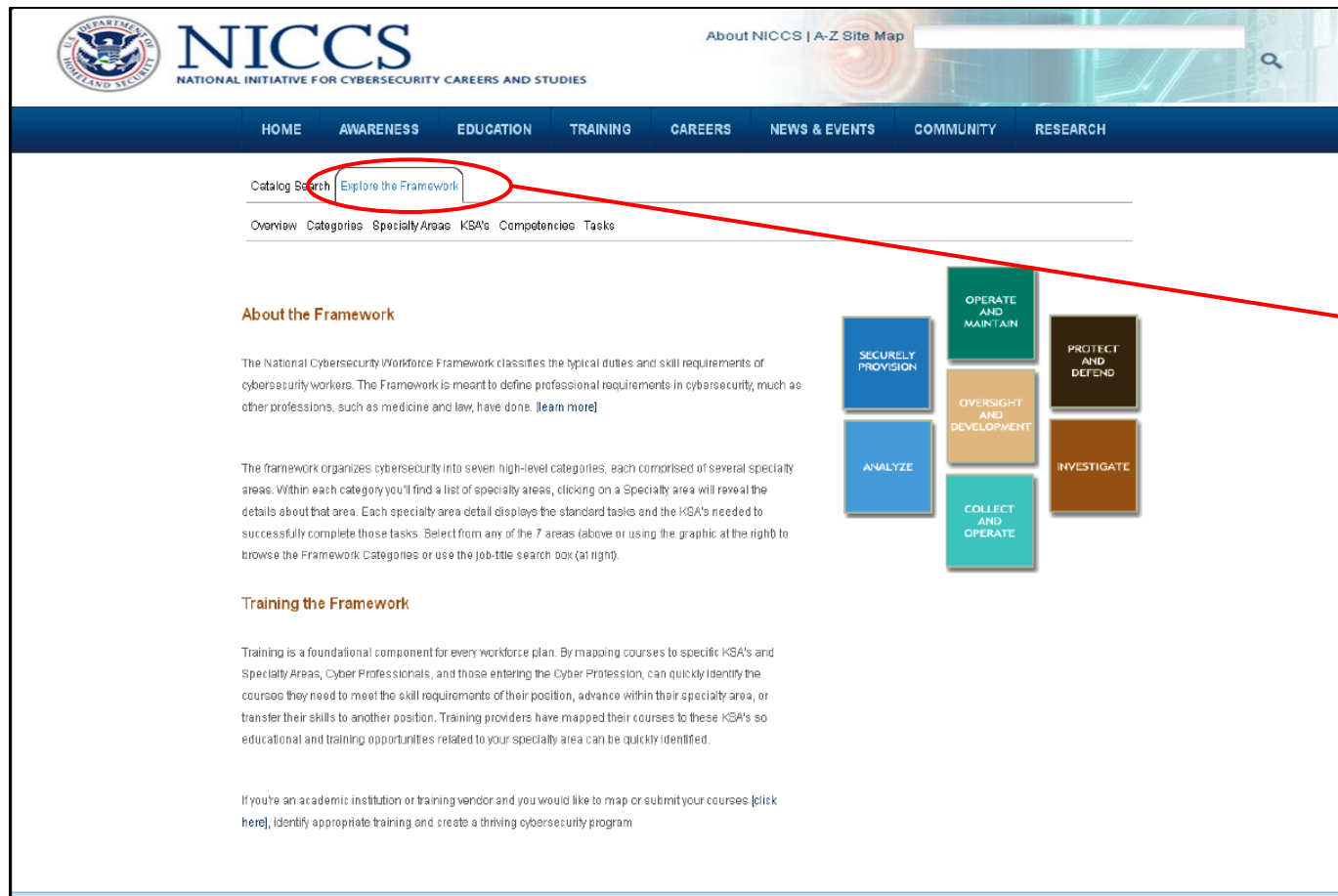
- Computer Forensics
- Encryption
- Information Assurance
- Information Systems/Network Security
- Infrastructure Design
- Vulnerabilities Assessment

Provider
<http://www.acme.org>
Contact
1-800-123-4567
info@acme.org

The Training information page provides the following information:

- **Description**
- **Provider**
- **Course Prerequisites**
- **Training Purpose**
- **Overall Course Level**
- **Audience**
- **Training Origin**
- **Learning Objectives**
- **Framework Categories and Competencies**

Navigating the Catalog: Explore the Framework



The screenshot shows the NICCS website interface. At the top, the NICCS logo and name are displayed. Below the navigation bar, the 'Catalog Search' section is visible, with the 'Explore the Framework' link highlighted by a red circle. A red arrow points from this link to the text on the right. The main content area includes sections for 'About the Framework', 'Training the Framework', and a central graphic showing seven high-level categories: Securely Provision, Operate and Maintain, Protect and Defend, Analyze, Oversight and Development, Investigate, and Collect and Operate.

About the Framework

The National Cybersecurity Workforce Framework classifies the typical duties and skill requirements of cybersecurity workers. The Framework is meant to define professional requirements in cybersecurity, much as other professions, such as medicine and law, have done. [\[learn more\]](#)

The framework organizes cybersecurity into seven high-level categories, each comprised of several specialty areas. Within each category you'll find a list of specialty areas, clicking on a Specialty area will reveal the details about that area. Each specialty area detail displays the standard tasks and the KSA's needed to successfully complete those tasks. Select from any of the 7 areas (above) or using the graphic at the right to browse the Framework Categories or use the job-title search box (at right).

Training the Framework

Training is a foundational component for every workforce plan. By mapping courses to specific KSA's and Specialty Areas, Cyber Professionals, and those entering the Cyber Profession, can quickly identify the courses they need to meet the skill requirements of their position, advance within their specialty area, or transfer their skills to another position. Training providers have mapped their courses to these KSA's so educational and training opportunities related to your specialty area can be quickly identified.

If you're an academic institution or training vendor and you would like to map or submit your courses [\[click here\]](#), identify appropriate training and create a thriving cybersecurity program

In addition to searching the Cybersecurity Training and Education Catalog, you can explore the National Cybersecurity Workforce Framework.

*To explore the Framework, click the tab to the right of the Catalog Search tab, **Explore the Framework.***

*You can explore the Framework by clicking on **Overview, Categories, Specialty Areas, KSAs, Competencies, and Skills.***

Navigating the Catalog: Explore the Framework Specialty Areas



The screenshot shows the NICCS (National Initiative for Cybersecurity Careers and Studies) Training Catalog. The 'Specialty Areas' tab is selected and highlighted with a red circle. A red arrow points from this tab to the 'Information Assurance Compliance' section. The page displays the following content:

- Information Assurance Compliance**
 - [Related Job Titles](#) | [Tasks](#) | [KSAs](#)
 - DESCRIPTION**
Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements. Ensures compliance from internal and external perspectives.
 - RELATED JOB TITLES**
Persons working in this Specialty Area may have job titles similar to:
 - Accreditor
 - Validator
 - IA Manager
 - IA Officer
 - Designated Accrediting Authority
 - Certifying Official
 - Certification Agent
 - IA Compliance Analyst/Manager
 - Auditor
 - Security Control Assessor
 - Authorizing Official Designated Representative
 - Risk/Vulnerability Analyst
 - Portfolio Manager
 - Compliance Manager
 - TASKS**
Professional involved in this Specialty perform the following tasks:
 - Develop methods to monitor and measure compliance
 - Develop specifications to ensure compliance with security requirements at the system or network environment level
 - Draft statements of preliminary or residual security risks for system operation
 - Maintain information systems accreditations
 - Manage and approve Accreditation Packages (e.g., Defense Information Assurance Certification and Accreditation Process, National Information Assurance Certification and Accreditation Process, etc.)

On the right side of the page, under 'Area Competency', there is a list of competencies:

- [Enterprise Architecture](#)
- [Information Assurance](#)
- [Information Systems Security Certification](#)
- [Information Systems/Network Security](#)
- [Information Technology Performance Assessment](#)
- [Infrastructure Design](#)
- [Legal, Government and Jurisprudence](#)
- [Logical Systems Design](#)
- [Systems Testing and Evaluation](#)

Initially, the Cybersecurity Training and Education Catalog training is mapped to the Framework Specialty Areas. In future phases of the Cybersecurity Training and Education Catalog, courses may also be mapped to Knowledge, Skills, and Abilities.

*You can explore the Workforce Specialty Areas by clicking the tab **Specialty Area**.*

Each specialty area page includes a description, related job titles, a list of sample tasks, and examples of KSAs.

How is Training Added to the Catalog?

The courses in the Cybersecurity Training and Education Catalog have been submitted by cybersecurity training providers. Next, we will explore how training can be added to the catalog.

- All training providers are invited to submit courses (although submissions are voluntary, and all information posted to the NICCS Portal is subject to certain criteria).
- The next few slides illustrate important NICCS links, and proceed through a recommended 4-step course inclusion process.

Let's get started...



Add Training to the Catalog

The screenshot shows the NICCS (National Initiative for Cybersecurity Careers and Studies) website. The top navigation bar includes links for HOME, AWARENESS, EDUCATION, TRAINING, CAREERS, NEWS & EVENTS, COMMUNITY, and RESEARCH. The TRAINING tab is highlighted with a red circle. Below the navigation bar, the TRAINING section is titled "Promoting Continuous Workforce Development". On the left, a sidebar menu lists: Training Home, Training Catalog, Call for Providers (circled in red), Map Your Training, National Cybersecurity Workforce Framework, Professional Certifications, FedVTE, and Workforce Development. The main content area features four primary actions: FIND COURSES (with a magnifying glass icon), GET CERTIFIED (with a "CERTIFIED" stamp icon), DEVELOP TRAINING (with a gear icon), and SUBMIT TRAINING (with a person icon and a red circle around the text "SUBMIT TRAINING"). Each action has a brief description. To the right of these actions are sections for "TRAINING RESOURCES FOR FEDERAL EMPLOYEES" and "PUBLIC TRAINING VENDORS". Red arrows point from the "Call for Providers" link in the sidebar to the text on the right, and from the "SUBMIT TRAINING" button to the text on the right.

Information about how to add your training courses to the Cybersecurity Training and Education Catalog is also available on the **TRAINING** tab.

On the training landing page, you can click either **“Call for Providers,”** or the **“Submit Training”** button to learn more.

The next few slides of this presentation will explain more about how to submit your training for inclusion in the Cybersecurity Training and Education Catalog.

Add Training to the Cybersecurity Training and Education Catalog: 4-Step Process



The success of the Cybersecurity Training and Education Catalog depends on the completeness and accuracy of information your organization provides.

To add your training to the Cybersecurity Training and Education Catalog, we suggest the following process:

1. **Apply** – Complete the NICCS Provider Template and send us your organization's contact information via email.
2. **Map** – Download the suggested training collection template, enter your training, and determine which of the Framework's specialty areas align to the training.
3. **Submit** – Submit your training to NICCS Supervisory Office by emailing the information to NICS@hq.dhs.gov.
4. **Verify** – Verify your training are posted properly and update them frequently.

Add Training to the Cybersecurity Training and Education Catalog: Apply



The first step to adding your training to the Cybersecurity Training and Education Catalog is to become an approved NICCS Training Provider. Every training provider is asked to review a set of established vetting criteria and provide responses. Once approved by the NICCS Supervisory Office (SO), subsequent training submissions to the Cybersecurity Training and Education Catalog will be processed quicker.

- Download the [NICCS Portal Provider Template](#).
- Return the requested information to the NICCS SO at NICS@hq.dhs.gov.
- You will receive an email confirming receipt. If the NICCS SO has any additional questions for you, they will reach out to you using the contact information you provided.
- Once approved, you will be sent a unique **NICCS Provider ID** to use with all future correspondence and training submissions.

Add Training to the Cybersecurity Training and Education Catalog: Map



Once you have received your unique **NICCS Provider ID**, you can begin compiling and preparing training information to submit to NICCS Supervisory Office (SO). As part of that process, you will need to map your training courses to a Framework Specialty Area(s), as well as provide training specific details.

- Download the [Cybersecurity Training Data Collection Template](#).
- Complete this form for training you would like to post. For example, you will be asked to provide the following Training Course information: Description, Catalog Number, URL, Purpose, Proficiency Level (see next slide), Audience, Learning Objectives, Prerequisites, and Delivery modality.
- Additionally, you will be able to map (i.e .associate) up to five Framework Specialty Area(s) to the training. Use the “**Explore the Framework**” links under the “**TRAINING**” tab on NICCS to determine which Specialty Areas most closely align to your courses.

Add Training to the Cybersecurity Training and Education Catalog: Map cont.



When you complete the [Cybersecurity Training Data Collection Form](#), you will be asked to select the training proficiency level for each course. This information will assist individuals in selecting the appropriate level of required training. The proficiency levels are defined below:

Level	Description
0	This training is intended for someone with insufficient knowledge, skill, or ability level necessary for use in simple or routine work situations. Knowledge, skill, or ability level provided would be similar to the knowledge of a layperson. Considered “no proficiency” for purposes of accomplishing specialized, or technical, work.
1	This training is intended for individuals who need basic knowledge, skills, or abilities necessary for use and the application in simple work situations with specific instructions and/or guidance.
2	This training is intended for individuals who need intermediate knowledge, skills, or abilities for independent use and application in straightforward, routine work situations with limited need for direction.
3	This training is intended for individuals who need advanced knowledge, skills, or abilities for independent use and application in complex or novel work situations.
4	This training is intended for individuals who need expert knowledge, skills, or abilities for independent use and application in highly complex, difficult, or ambiguous work situations, or the trainee is an acknowledged authority, advisor, or key resource.

Add Training to the Cybersecurity Training and Education Catalog: Submit



Once the Cybersecurity Training Data Collection Form is complete, please submit to the NICCS Supervisory Office (SO).

- The form can be submitted to NICS@hq.dhs.gov.
- You should receive a confirmation that your form was received by the NICCS SO.
- Deadlines for course submissions:
 - February 6 – Courses for March Catalog Release (Federal training providers)
 - April 24 – Courses for June Catalog Release
 - July 24 – Courses for September Catalog Release
- The NICCS SO may contact you to request additional information.

Add Training to the Cybersecurity Training and Education Catalog: Verify



Lastly, please verify and update your data on an ongoing basis.

- You will receive notification when your training has been uploaded to the Cybersecurity Training and Education Catalog.
- At that time, you can verify your training is described accurately and your provider contact information is correct.
- To maintain accuracy of the data, we strongly suggest you review your training on a regular basis and submit updated information routinely.

How will the Information be Monitored?

The NICCS Portal, and the Cybersecurity Training and Education Catalog, are monitored by the NICCS Supervisory Office (SO). The SO is responsible for the following:

- Responding to emails to the NICCS SO general mailbox.
- Reviewing the website daily to fix any errors or to edit inaccurate information.
- Updating the site with timely information and additional cybersecurity training and education information.
- Partnering with cybersecurity training providers to help post training to the Cybersecurity Training and Education Catalog.
- If you notice any that needs to be fixed on the website, please let us know!
You can email us at NICS@hq.dhs.gov.



We need your help!

- The success of the Cybersecurity Training and Education Catalog depends on your support.
- Your input is valuable. Would you like to see anything else added to the Training Catalog with future versions?
- To make this as comprehensive a resource as possible, please help us by submitting your training by following the 4-step process described throughout this presentation.
- For any questions or concerns, please use the NICCS SO mailbox: NICS@hq.dhs.gov.
- **Visit NICCS here:** <http://niccs.us-cert.gov/>

